Claims:

1   1.   A mobile application security system, comprising:

2   a management and security console computer that executes instructions for controlling

3   the security of a mobile application;

4   one or more host computers connected to the console computer, each host computer

5   executing the mobile application that jumps between the hosts during execution;

6   the console computer further comprising means for monitoring the security of the mobile

7   application as it jumps between a dispatching host and another host wherein information about

8   the mobile application and the dispatching host is communicated to the console computer; and

9   wherein the security monitoring means further comprises means for determining if

10   authentication of the dispatching host is required prior to dispatch of the mobile application.

11   2.   The system of Claim 1, wherein the determining means further comprises means

12   for determining if the mobile application being dispatched is a sensitive application, means for

13   determining if the dispatching host is vulnerable and means for requesting authentication if a

14   sensitive mobile application is being dispatched from a vulnerable host.

1   3.   The system of Claim 1, wherein the determining means further comprises means

2   for determining if the mobile application being dispatched is a sensitive application and means

3   for requesting authentication if a sensitive mobile application is being dispatched.

1   4.   The system of Claim 1, wherein the determining means further comprises means

2   for determining if the dispatching host is vulnerable and means for requesting authentication if a

3   mobile application is being dispatched from a vulnerable host.

1   5.   The system of Claim 1, wherein the determining means further comprises means

2   for authenticating the dispatching host based on one or more rules defined by an operator of the

3   system.

1   6.   The system of Claim 2, wherein the determining means further comprises means

2   for assigning a vulnerable classification or a non-vulnerable classification to each host in the

3   mobile application system.

1   7.   The system of Claim 2, wherein the determining means further comprises means

2   for assigning a sensitive classification or a non-sensitive classification to each mobile application

3   in the mobile application system as the mobile application is created.

     8.   The system of Claim 1, wherein each mobile application comprises an itinerary

listing a node for each host to which the mobile application jumps in the mobile application

system wherein each node indicates if authentication is required to jump from the particular host

and wherein the determining means further comprises means for requesting authentication based

on the node in the itinerary.

     9.   The system of Claim 2, wherein the host comprises one or more wireless device

that are classified as vulnerable.

1   10.   A mobile application security method, comprising:

2   receiving data about a mobile application at a security node each time the mobile

3   application jumps from a dispatching host to another host in a mobile application system; and

4   determining if authentication of the dispatching host is required prior to dispatch of the

5   mobile application.

1   11.   The method of Claim 10, wherein determining further comprises determining if

2   the mobile application being dispatched is a sensitive application, determining if the dispatching

3   host is vulnerable and requesting authentication if a sensitive mobile application is being

4   dispatched from a vulnerable host.

1   12.   The method of Claim 10, wherein determining further comprises determining if

2   the mobile application being dispatched is a sensitive application and requesting authentication if

3   a sensitive mobile application is being dispatched.

1   13.   The method of Claim 10, wherein determining further comprises determining if

2   the dispatching host is vulnerable and requesting authentication if a mobile application is being

3   dispatched from a vulnerable host.

1   14.   The method of Claim 10, wherein determining further comprises authenticating

2   the dispatching host based on one or more rules defined by an operator of the method.

1   15.   The method of Claim 11, wherein determining further comprises assigning a

2   vulnerable classification or a non-vulnerable classification to each host in the mobile application

3   method.

1   16.   The method of Claim 11, wherein determining further comprises assigning a

2   sensitive classification or a non-sensitive classification to each mobile application in the mobile

3   application system as the mobile application is created.

1   17.   The method of Claim 10, wherein each mobile application comprises an itinerary

2   listing a node for each host to which the mobile application jumps in the mobile application

3   system wherein each node indicates if authentication is required to jump from the particular host

4   and wherein the determining further comprises requesting authentication based on the node in the

5   itinerary.

1   18.   The method of Claim 11, wherein the host comprises one or more wireless device

2   that are classified as vulnerable.

1   19.   A mobile application security system, comprising:

2   one or more nodes of a peer-to-peer network wherein each node is configured to execute

3   a mobile application;

4   a management and security node connected to each node of the peer-to-peer network for

5   controlling the security of a mobile application;

6   the management and security node further comprising means for monitoring the security

7   of the mobile application as it jumps between the nodes wherein data about the mobile

8   application is communicated to the management and security node prior to the mobile

9   application being dispatched from a dispatching node; and

10   wherein the security monitoring means further comprises means for determining if

11   authentication of the dispatching node is required prior to dispatch of the mobile application.

20.   The system of Claim 19, wherein the determining means further comprises means

for determining if the mobile application being dispatched is a sensitive application, means for

determining if the dispatching node is vulnerable and means for requesting authentication if a

sensitive mobile application is being dispatched from a vulnerable node.

21.   The system of Claim 19, wherein the determining means further comprises means

for determining if the mobile application being dispatched is a sensitive application and means

for requesting authentication if a sensitive mobile application is being dispatched.

1   22.   The system of Claim 19, wherein the determining means further comprises means

2   for determining if the dispatching node is vulnerable and means for requesting authentication if a

3   mobile application is being dispatched from a vulnerable node.

1   23.   The system of Claim 19, wherein the determining means further comprises means

2   for authenticating the dispatching node based on one or more rules defined by an operator of the

3   system.

1   24.   The system of Claim 20, wherein the determining means further comprises means

2   for assigning a vulnerable classification or a non-vulnerable classification to each node in the

3   mobile application system.

1   25.   The system of Claim 20, wherein the determining means further comprises means

2   for assigning a sensitive classification or a non-sensitive classification to each mobile application

3   in the mobile application system as the mobile application is created.

1   26.   The system of Claim 19, wherein each mobile application comprises an itinerary

2   listing a node for each node to which the mobile application jumps in the mobile application

3   system wherein each node indicates if authentication is required to jump from the particular node

4   and wherein the determining means further comprises means for requesting authentication based

5   on the node in the itinerary.

27.   The system of Claim 20, wherein the host comprises one or more wireless device

that are classified as vulnerable.

28.   A mobile application security method, comprising:

receiving data about a mobile application at a management and security node each time

the mobile application is being dispatched from a dispatching node in a peer-to-peer network;

4   and

5   monitoring the security of the mobile application as it jumps between the nodes, wherein

6   the security monitoring further comprises determining if authentication of the dispatching node is

7   required prior to dispatch of the mobile application.

1   29.   The method of Claim 28, wherein determining further comprises determining if

2   the mobile application being dispatched is a sensitive application, determining if the dispatching

3   node is vulnerable and requesting authentication if a sensitive mobile application is being

4   dispatched from a vulnerable node.

1   30.   The method of Claim 28, wherein the determining further comprises determining

2   if the mobile application being dispatched is a sensitive application and requesting authentication

3   if a sensitive mobile application is being dispatched.

1   31.   The method of Claim 28, wherein the determining further comprises determining

2   if the dispatching node is vulnerable and requesting authentication if a mobile application is

3   being dispatched from a vulnerable node.

1   32.   The method of Claim 28, wherein the determining further comprises

2   authenticating the dispatching node based on one or more rules defined by an operator of the

3   system.

1   33.   The method of Claim 29, wherein the determining further comprises assigning a

2   vulnerable classification or a non-vulnerable classification to each node in the mobile application

3   system.

1   34.   The method of Claim 29, wherein the determining further comprises assigning a

2   sensitive classification or a non-sensitive classification to each mobile application in the mobile

3   application system as the mobile application is created.

1   35.   The method of Claim 28, wherein each mobile application comprises an itinerary

2   listing a node for each node to which the mobile application jumps in the mobile application

3   system wherein each node indicates if authentication is required to jump from the particular node

4   and wherein the determining further comprises requesting authentication based on the node in the

5   itinerary.

1   36.   The method of Claim 29, wherein the host comprises one or more wireless device

2   that are classified as vulnerable.